

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-271318

(43)Date of publication of application : 20.09.2002

(51)Int.Cl.

H04L 9/32
H04L 9/08
H04L 12/28

(21)Application number : 2001-062084

(71)Applicant : MITSUBISHI MATERIALS CORP

(22)Date of filing : 06.03.2001

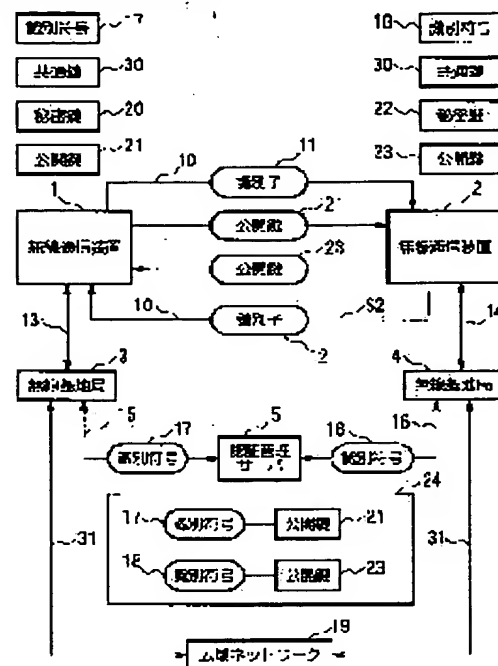
(72)Inventor : KURAMOTO EITARO

(54) RADIO COMMUNICATION EQUIPMENT AND CERTIFICATION MANAGING SERVER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide radio communication equipment which can inform an IP address to a communication partner without being known by outsiders.

SOLUTION: Radio communication equipment 1 transmits an identifier 11 to radio communication equipment 2 with a short distance communication part, and receives an identifier 12 of the radio communication equipment 2 therefrom. A common key producing part produces a common key 30 by using the identifier 11 and the received identifier 12. A key producing part produces a disclosure key 21 and a secret key 20 by using an identification code 11 of the radio communication equipment 1 which is issued from a radio base station 3 and the common key 30. A control unit transmits the disclosed key 21 to the radio communication equipment 2 with the short distance communication part. When communication is performed to the communication equipment, the control unit transmits a disclosed key 23 received from the radio communication equipment 2 to a certification managing server 5 as a communication destination, and receives an identification code 17 of the radio communication equipment 2 from the certification managing server 5.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-271318
(P2002-271318A)

(43) 公開日 平成14年9月20日 (2002.9.20)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 L 9/32		H 0 4 L 12/28	3 0 0 Z 5 J 1 0 4
9/08		9/00	6 7 3 B 5 K 0 3 3
12/28	3 0 0		6 0 1 D
			6 0 1 E
			6 0 1 F

審査請求 未請求 請求項の数10 O L (全 11 頁)

(21) 出願番号 特願2001-62084(P2001-62084)

(22) 出願日 平成13年3月6日(2001.3.6)

(71) 出願人 00006264

三菱マテリアル株式会社

東京都千代田区大手町1丁目5番1号

(72) 発明者 倉本 英太郎

東京都文京区小石川一丁目12番14号 三菱
マテリアル株式会社移動体事業開発センタ
ー内

(74) 代理人 100064908

弁理士 志賀 正武 (外6名)

Fターム(参考) 5J104 AA03 AA07 AA09 AA16 EA04

EA16 EA26 KA02 LA06 MA01

NA02 PA07

5K033 AA08 CB01 CC01 DA06 DA19

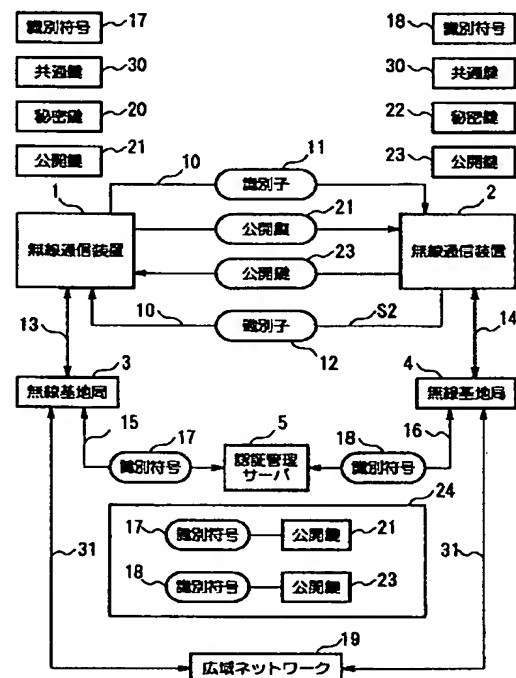
DB04 DB18 EA07 EC01 EC03

(54) 【発明の名称】 無線通信装置、認証管理サーバ

(57) 【要約】

【課題】 IPアドレスを第3者に知られないように通信相手に通知することができる無線通信装置を提供する。

【解決手段】 無線通信装置1は、近距離通信部によって識別子11を無線通信装置2に送信し、無線通信装置2の識別子12を無線通信装置2から受信する。共通鍵生成部は、識別子11と受信した識別子12とによって共通鍵30を生成する。鍵生成部は、無線基地局3から発行される無線通信装置1の識別符号11と共通鍵30とによって公開鍵21と秘密鍵20を生成する。そして、制御部は、近距離通信部によって公開鍵21を無線通信装置2に送信する。また、制御部は、無線通信装置2に対して通信を行う場合に、無線通信装置2から受信した公開鍵23を通信先として認証管理サーバ5に送信し、認証管理サーバ5から無線通信装置2の識別符号17を受信する。



【特許請求の範囲】

【請求項1】 少なくとも2経路の通信回線を介して他の無線通信装置に接続される通信システムにおける無線通信装置であって、

第1の通信回線を用いて通信相手となる無線通信装置の登録に関する通信を行う第1の通信手段と、

前記第1の通信手段によって登録された通信相手に対し、前記第1の通信回線と異なる通信回線を用いて通信を行う第2の通信手段と、

を有することを特徴とする無線通信装置。

【請求項2】 前記第1の通信手段は、登録を行う無線通信装置に対して近距離において登録に関する通信を行うことを特徴とする請求項1に記載の無線通信装置。

【請求項3】 少なくとも2経路の通信回線を介して他の無線通信装置に接続される通信システムにおける無線通信装置であって、

自身に設定された識別子を送信するとともに、通信を行う相手側の無線通信装置に設定された識別子を受信する第1の通信手段と、

前記自身に設定される識別子と前記第1の通信手段によって受信する相手側の無線通信装置に設定された識別子とに基づいて、共通鍵を生成する共通鍵生成手段と、

前記共通鍵生成手段によって生成される共通鍵と自身に設定される識別符号とに基づいて公開鍵を生成する公開鍵生成手段と、

前記公開鍵生成手段によって生成される公開鍵を前記第1の通信手段によって前記相手側の無線通信装置に送信するとともに、前記相手側の無線通信装置によって生成された公開鍵を前記相手側の無線通信装置から前記第1の通信手段によって受信して、通信相手として登録する制御手段と、

前記制御手段によって登録された通信相手となる無線通信装置に対し、前記公開鍵生成手段によって生成される公開鍵を用いて前記第1の通信手段とは異なる通信回線を用いて通信を行う第2の通信手段と、

を有することを特徴とする無線通信装置。

【請求項4】 前記第1の通信手段は、近距離において通信を行うことを特徴とする請求項3に記載の無線通信装置。

【請求項5】 少なくとも2台以上の無線通信装置と認証管理サーバとが接続される通信システムにおける認証管理サーバであって、

無線通信装置から送信される固有情報と識別符号との対応関係と、通信相手として信頼関係の確立がなされた無線通信装置同士の対応関係とを認証データとして記憶する記憶手段と、

通信相手となる無線通信装置を指定する固有情報を前記無線通信装置から通信要求として受信した場合、前記受信した固有情報に対応する識別符号を前記記憶手段に記憶された認証データから読み出し、読み出した識別符号

を前記通信要求を行った無線通信装置に送信する制御を行う制御手段とを有することを特徴とする認証管理サーバ。

【請求項6】 前記制御手段は、信頼関係の確立がなされていない無線通信装置間で通信を行う相手側の無線通信装置の登録を行う場合に、

前記記憶手段に記憶された認証データに基づいて、前記信頼関係の確立がなされていない無線通信装置同士が共通に信頼関係の確立を行っている無線通信装置を介し、

通信を行う相手側の無線通信装置の登録を行うように制御することを特徴とする請求項5に記載の認証管理サーバ。

【請求項7】 前記固有情報は、無線通信装置によって生成される公開鍵であることを特徴とする請求項5または請求項6に記載の認証管理サーバ。

【請求項8】 少なくとも2経路の通信回線を介して他の無線通信装置に接続される通信システムにおける無線通信装置における通信相手登録プログラムを記録した記録媒体であって、

前記記録媒体は、

自身に設定された識別子を送信するとともに、通信を行う相手側の無線通信装置に設定された識別子を受信する第1の通信ステップと、

前記自身に設定される識別子と前記受信する識別子とに基づいて共通鍵を生成する共通鍵生成ステップと、

前記共通鍵生成ステップによって生成される共通鍵と自身に設定される識別符号とに基づいて公開鍵を生成する公開鍵生成ステップと、

前記公開鍵生成ステップによって生成される公開鍵を前記第1の通信ステップにおける通信回線を介して前記相手側の無線通信装置に送信する送信ステップと、

前記相手側の無線通信装置によって生成された公開鍵を前記相手側の無線通信装置から前記第1の通信ステップにおける通信回線を用いて受信して、通信相手として登録する登録ステップと、

前記登録ステップによって登録された通信相手となる無線通信装置に対し、前記公開鍵生成ステップによって生成される公開鍵を用いて前記第1の通信ステップにおける通信回線とは異なる通信回線を用いて通信を行う第2の通信ステップと、

をコンピュータに実行させるための通信相手登録プログラムを記録したことを特徴とする記録媒体。

【請求項9】 少なくとも2台以上の無線通信装置と認証管理サーバとが接続される通信システムにおける認証管理サーバにおける通信プログラムを記録した記録媒体であって、

前記記録媒体は、

無線通信装置から送信される固有情報と識別符号との対応関係と、通信相手として信頼関係の確立がなされた無線通信装置同士の対応関係とを認証データとして記憶す

る記憶ステップと、
通信相手となる無線通信装置を指定する固有情報を前記無線通信装置から通信要求として受信した場合、前記記憶ステップにおいて記憶された認証データに基づいて、前記受信した固有情報に対応する識別符号を前記通信要求を行った無線通信装置に送信する制御を行う制御ステップとをコンピュータに実行させる通信プログラムを記録したことを特徴とする記録媒体。

【請求項10】 少なくとも2経路の通信回線を介して他の無線通信装置に接続される通信システムにおける通信方法であって、

第1の通信回線を用いて通信相手となる無線通信装置の登録に関する通信を行い、前記登録された通信相手に対し、前記第1の通信回線と異なる通信回線を用いて通信を行うことを特徴とする通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、無線によって通信を行う無線通信装置に係り、特に、無線通信装置に設定される識別符号の秘匿性を向上させて通信を行う無線通信装置に関するものである。

【0002】

【従来の技術】従来から、通信相手となる端末と自身の端末との相互間において、インターネット等のネットワークを介して、データの送受信を行う方法が知られている。通信したい相手に、自身のアドレス（IPアドレス、メールアドレス、電話番号等）を教える場合、例えば、端末の利用者は、通信相手に自分のアドレスを口頭で伝えたり、アドレスを記入したメモを通信相手に渡す等していた。

【0003】

【発明が解決しようとする課題】しかしながら、従来は、口頭でアドレスを通信相手に教える場合、近くにいる第三者によってアドレスが聞き取られると、アドレスを教えた相手以外にアドレスが知られてしまう可能性があった。また、従来は、アドレスを記入したメモを相手に渡す場合、メモに書かれたアドレスが、第三者によって見られてしまい、アドレスを教えた相手以外にアドレスが知られてしまう可能性があった。例えば、上述した状況下において、悪意ある第三者にアドレスが知られてしまうと、この悪意ある第三者からDoS攻撃を受ける可能性がある。ここで、DoS攻撃とは、インターネット経由でサーバやシステムに過負荷をかけてサービス停止に追い込む行為のことをいう。このように、従来においては、アドレスなどの端末固有の識別符号を通信相手に教える場合に、アドレスが第三者に漏洩してしまうという問題点があった。

【0004】本発明は、このような事情に鑑みてなされたもので、その目的は、識別符号であるIPアドレスを第三者に知られないように通信相手に通知することがで

きる無線通信装置を提供することにある。

【0005】

【課題を解決するための手段】上記目的を達成するために、本発明は、少なくとも2経路の通信回線を介して他の無線通信装置に接続される通信システムにおける無線通信装置であって、第1の通信回線を用いて通信相手となる無線通信装置の登録に関する通信を行う第1の通信手段（例えば、実施の形態における近距離通信部）と、前記第1の通信手段によって登録された通信相手に対し、前記第1の通信回線と異なる通信回線を用いて通信を行う第2の通信手段（例えば、実施の形態における遠距離通信部）とを有することを特徴とする。

【0006】また、本発明は、上述の無線通信装置において、前記第1の通信手段は、登録を行う無線通信装置に対して近距離において登録に関する通信を行うことを特徴とする。

【0007】また、本発明は、少なくとも2経路の通信回線を介して他の無線通信装置に接続される通信システムにおける無線通信装置であって、自身に設定された識別子を送信するとともに、通信を行う相手側の無線通信装置に設定された識別子を受信する第1の通信手段と、前記自身に設定される識別子と前記第1の通信手段によって受信する相手側の無線通信装置に設定された識別子とに基づいて、共通鍵を生成する共通鍵生成手段（例えば、実施の形態における共通鍵生成部151）と、前記共通鍵生成手段によって生成される共通鍵と自身に設定される識別符号とに基づいて公開鍵を生成する公開鍵生成手段（例えば、実施の形態における鍵生成部）と、前記公開鍵生成手段によって生成される公開鍵を前記第1の通信手段によって前記相手側の無線通信装置に送信するとともに、前記相手側の無線通信装置によって生成された公開鍵を前記相手側の無線通信装置から前記第1の通信手段によって受信して、通信相手として登録する制御手段（例えば、実施の形態における制御部160）と、前記制御手段によって登録された通信相手となる無線通信装置に対し、前記公開鍵生成手段によって生成される公開鍵を用いて前記第1の通信手段とは異なる通信回線を用いて通信を行う第2の通信手段とを有することを特徴とする。

【0008】また、本発明は、上述の無線通信装置において、前記第1の通信手段は、近距離において通信を行うことを特徴とする。

【0009】また、本発明は、少なくとも2台以上の無線通信装置と認証管理サーバとが接続される通信システムにおける認証管理サーバであって、無線通信装置から送信される固有情報と識別符号との対応関係と、通信相手として信頼関係の確立がなされた無線通信装置同士の対応関係とを認証データとして記憶する記憶手段（例えば、実施の形態における記憶部5-2）と、通信相手となる無線通信装置を指定する固有情報を前記無線通信装

置から通信要求として受信した場合、前記受信した固有情報に対応する識別符号を前記記憶手段に記憶された認証データから読み出し、読み出した識別符号を前記通信要求を行った無線通信装置に送信する制御を行う制御手段（例えば、実施の形態における制御部5-3）とを有することを特徴とする。

【0010】また、本発明は、上述の認証管理サーバにおいて、前記制御手段は、信頼関係の確立がなされていない無線通信装置間で通信を行う相手側の無線通信装置の登録を行う場合に、前記記憶手段に記憶された認証データに基づいて、前記信頼関係の確立がなされていない無線通信装置同士が共通に信頼関係の確立を行っている無線通信装置を介し、通信を行う相手側の無線通信装置の登録を行うように制御することを特徴とする。

【0011】また、本発明は、上述の認証管理サーバにおいて、前記固有情報は、無線通信装置によって生成される公開鍵であることを特徴とする。

【0012】また、本発明は、少なくとも2経路の通信回線を介して他の無線通信装置に接続される通信システムにおける無線通信装置における通信相手登録プログラムを記録した記録媒体であって、前記記録媒体は、自身に設定された識別子を送信するとともに、通信を行う相手側の無線通信装置に設定された識別子を受信する第1の通信ステップと、前記自身に設定される識別子と前記受信する識別子とに基づいて共通鍵を生成する共通鍵生成ステップと、前記共通鍵生成ステップによって生成される共通鍵と自身に設定される識別符号とに基づいて公開鍵を生成する公開鍵生成ステップと、前記公開鍵生成ステップによって生成される公開鍵を前記第1の通信ステップにおける通信回線を介して前記相手側の無線通信装置に送信する送信ステップと、前記相手側の無線通信装置によって生成された公開鍵を前記相手側の無線通信装置から前記第1の通信ステップにおける通信回線を用いて受信して、通信相手として登録する登録ステップと、前記登録ステップによって登録された通信相手となる無線通信装置に対し、前記公開鍵生成ステップによって生成される公開鍵を用いて前記第1の通信ステップにおける通信回線とは異なる通信回線を用いて通信を行う第2の通信ステップと、をコンピュータに実行させるための通信相手登録プログラムを記録したことを特徴とする。

【0013】また、本発明は、少なくとも2台以上の無線通信装置と認証管理サーバとが接続される通信システムにおける認証管理サーバにおける通信プログラムを記録した記録媒体であって、前記記録媒体は、無線通信装置から送信される固有情報と識別符号との対応関係と、通信相手として信頼関係の確立がなされた無線通信装置同士の対応関係とを認証データとして記憶する記憶ステップと、通信相手となる無線通信装置を指定する固有情報を前記無線通信装置から通信要求として受信した場

合、前記記憶ステップにおいて記憶された認証データに基づいて、前記受信した固有情報に対応する識別符号を前記通信要求を行った無線通信装置に送信する制御を行う制御ステップとをコンピュータに実行させる通信プログラムを記録したことを特徴とする。

【0014】また、本発明は、少なくとも2経路の通信回線を介して他の無線通信装置に接続される通信システムにおける通信方法であって、第1の通信回線を用いて通信相手となる無線通信装置の登録に関する通信を行い、前記登録された通信相手に対し、前記第1の通信回線と異なる通信回線を用いて通信を行うことを特徴とする。

【0015】

【発明の実施の形態】以下、本発明の一実施形態による無線通信装置を図面を参照して説明する。図1は、この発明の一実施形態による無線通信装置、認証サーバを適用した通信システムの構成を示す概略ブロック図である。この図において、無線通信装置1および無線通信装置2は、第1の通信回線または第2の通信回線を介して相互に通信を行う。また、無線通信装置1は、端末1-1～端末1-nと通信を行い、無線通信装置2は、端末2-1～端末2-mと通信を行う。

【0016】10は、無線通信装置1および無線通信装置2とを接続し、無線通信装置に設定された識別符号の伝送する近距離通信回線である。この近距離通信回線10が、第1の通信回線に対応する。この第1の通信回線としては、例えば、赤外線通信やBLUETOOTH（近距離無線通信技術）等の無線あるいは接続ケーブルなどの有線によって無線通信装置間を接続するものである。以下、第1の通信回線を介して行う通信を近距離通信と称する。ここでは、例えば、BLUETOOTHが近距離通信回線10として適用される。

【0017】無線基地局3および無線基地局4は、広域ネットワーク19を介して相互通信可能に接続される。ここでは、広域ネットワーク19を介して行う通信を遠距離通信と称する。また、無線基地局3および無線基地局4は、無線によって無線通信装置1または無線通信装置2に接続されるとともに、必要に応じて無線通信装置に識別符号を動的に割り当てる。

【0018】認証管理サーバ5は、相互に信頼関係を確立した各無線通信装置間の対応関係を示す認証データを記憶する（詳細は後述する）。また、認証管理サーバ5は、公開鍵と公開鍵の利用者に関する情報に基づいて、申請内容のチェックを行い、認証局の電子署名付公開鍵を発行する。

【0019】13、14は、認証データおよび通信データを伝送する通信回線である。この通信回線13および通信回線14は、無線によって無線通信装置と無線基地局を接続する。15、16は、相互認証情報を登録、参照するための通信回線である。31は、広域ネットワー

ク19と無線基地局3、無線基地局4とを接続する通信回線である。広域ネットワーク19は、例えば、インターネット等のネットワークである。この広域ネットワーク19を用いる通信回線が第2の通信回線に対応している。すなわち、無線通信装置1と無線通信装置2との間は、第2の通信回線である広域ネットワーク19を用いるとともに、通信回線13、無線基地局3、通信回線31、無線基地局4、通信回線14を用いて接続される。

【0020】次に、無線通信装置1について、図2を用いてさらに詳細に説明する。図2は、無線通信装置1の構成を示す概略ブロック図である。この図に示すように、無線通信装置1の通信部100は、近距離通信部110と遠距離通信部130とによって構成され、近距離通信回線10（ここでは、BLUETOOTH）を用いて通信相手となる無線通信装置の登録に関する通信を行う。

【0021】近距離通信部110は、近距離通信回線10を介して通信相手となる無線通信装置2と近距離における通信を行う。ここで、近距離における通信とは、近距離通信部110が通信可能な領域内であり、例えば、通信を行う相手側の無線通信装置の使用者を視覚によって確認できる距離である。また、近距離通信部110は、BLUETOOTHによって端末1-1～端末1-nと通信を行う。なお、近距離通信部110と端末1-1～端末1-nは、赤外線通信等の無線あるいは接続ケーブルなどの有線によって接続されてもよい。遠距離通信部130は、無線によって無線基地局3と接続し、広域ネットワーク19に接続される。

【0022】記憶部140は、自身に設定される識別子11を記憶する。この識別子は、無線通信装置1に予め設定される。例えば、この識別子は、IPアドレス、MACアドレス（物理アドレス）等である。また、記憶部140は、制御部160からの指示に応じて、各種データを記憶する。

【0023】鍵生成部150は、共通鍵生成部151を有する。共通鍵生成部151は、識別子11と近距離通信回線10を介して送信される通信を行う相手側の無線通信装置（例えば、無線通信装置2）に設定される識別符号（例えば、識別子12）とに基づいて、共通鍵30を生成する。この共通鍵30は、識別子11と識別子12とに基づいて、一意に算出される値である。

【0024】また、鍵生成部150は、共通鍵生成部151によって生成される共通鍵30と無線基地局（例えば、無線基地局3）から設定される識別符号（例えば、識別符号17）とに基づいて、秘密鍵と公開鍵（秘密鍵20と公開鍵21）とを生成する。この識別符号は、例えば、IPアドレスであり、無線基地局から設定される。

【0025】制御部160は、鍵生成部150によって生成される公開鍵を近距離通信部110によって相手側

の無線通信装置に送信するとともに、相手側の無線通信装置によって生成された公開鍵を相手側の無線通信装置から近距離通信部110によって受信して、通信相手として登録する制御を行う。また、制御部160は、鍵生成部150によって生成される公開鍵（例えば、公開鍵21）を用いて、遠距離通信部130によって広域ネットワーク19と接続し、通信を行う制御をする。また、制御部160は、共通鍵生成部151によって生成される共通鍵（例えば、共通鍵30）を用いて、信頼関係が確立（詳細は後述する）された無線通信装置に対し、近距離通信部110によって通信を行う。

【0026】なお、図1における無線通信装置2は、無線通信装置1における記憶部140に自身に設定される識別子12を記憶している以外において、無線通信装置1と同様の構成を有する。

【0027】次に、図1における認証管理サーバ5について図3を用いてさらに詳細に説明する。図3は、認証管理サーバ5の構成を示す概略ブロック図である。この図において、認証管理サーバ5は、通信部5-1と、記憶部5-2と、制御部5-3によって構成される。通信部5-1は、広域ネットワーク19と無線基地局を介して無線通信装置と通信を行う。

【0028】記憶部5-2は、図5に示すように、無線通信装置から送信される固有情報（公開鍵）と識別符号との対応関係と、通信相手として信頼関係の確立がなされた無線通信装置同士の対応関係とを認証データとして記憶する。制御部5-3は、記憶部5-2に記憶されている認証データに基づいて、無線通信装置から送信される送信先を示す公開鍵に対応する識別符号を読み出し、読み出した識別符号を通信要求を行った無線通信装置に送信する制御を行う。

【0029】次に、図2の構成における無線通信装置と図3の構成における認証管理サーバを適用した通信システムの動作について、図2、図3、図4、図5を用いて説明する。ここでは、無線通信装置1と無線通信装置2とが信頼関係の確立を行った後に、遠距離通信回線（第2の通信回線）を用いて通信を行う場合について説明する。また、識別子11が予め無線通信装置1に設定され、無線通信装置1の記憶部140に記憶されており、識別子12が予め無線通信装置2に設定され、無線通信装置2の記憶部140に記憶されているものとする。

【0030】まず、無線通信装置1を携帯した使用者と無線通信装置2を携帯した使用者とが近距離通信回線10によって通信可能な距離内に近づき、近距離通信部110によって相互に接続する。次に、無線通信装置1は、近距離通信部110によって識別子11を無線通信装置2に送信し、無線通信装置2から送信される識別子12を受信する。次いで、無線通信装置1は、識別子11と無線通信装置2から受信した識別子12とに基づき、共通鍵生成部151によって共通鍵30を生成す

る。さらに、無線通信装置1は、遠距離通信部130によって無線基地局3に接続し、識別符号の発行要求を行い、無線基地局3から発行される識別符号17を受信し、記憶部140に記憶する。そして、無線通信装置1は、共通鍵30と識別符号17とに基づき、鍵生成部150によって公開鍵21とこの公開鍵21に対応する秘密鍵20とを生成し、記憶部140に記憶する。

【0031】一方、無線通信装置2は、無線通信装置1と同様に、近距離通信部110によって識別子11を無線通信装置2に送信すると、無線通信装置1から送信される識別子12と識別子11とに基づき、共通鍵生成部151によって共通鍵30を生成する。次いで、無線通信装置2は、遠距離通信部130によって無線基地局4に接続し、識別符号の発行要求を行い、無線基地局3から発行される識別符号18を受信し、記憶部140に記憶する。そして、無線通信装置2は、共通鍵30と識別符号18とに基づき、鍵生成部150によって公開鍵23とこの公開鍵23に対応する秘密鍵22とを生成し、記憶部140に記憶する。

【0032】次に、無線通信装置1は、遠距離通信部130によって認証管理サーバ5に公開鍵21と無線通信装置1の利用者に関する情報とを送信し、認証管理サーバ5によって発行される電子署名が付与された公開鍵21を受信して記憶部140に記憶する。一方、無線通信装置2も同様に、認証管理サーバ5から発行される電子署名が付与された公開鍵23が記憶される。

【0033】上述の処理がなされた後、無線通信装置1の制御部160は、近距離通信部110によって電子署名が付与された公開鍵21を無線通信装置2に送信し、無線通信装置2から送信される電子署名が付与された公開鍵23を受信して記憶部140に記憶する。これにより、無線通信装置1において、公開鍵23が、公開鍵に付与された電子署名により、正当性が確認される。また、無線通信装置2において、公開鍵21が、公開鍵に付与された電子署名により、正当性が確認される。

【0034】一方、認証管理サーバ5は、無線通信装置1に対して電子署名が付与された公開鍵21を発行する場合に、電子署名が付与された公開鍵21と無線通信装置1の識別符号17とを対応づけて記憶部5-2に認証データとして記憶するとともに、無線通信装置2に対して電子署名が付与された公開鍵23を発行する場合に、電子署名が付与された公開鍵23と無線通信装置2の識別符号18とを対応づけて認証データとして記憶部5-2に記憶する。このとき、記憶部5-2には、例えば、図5に示すような認証データが記憶される。

【0035】上述の処理が完了することにより、無線通信装置1と無線通信装置2との間において信頼関係の確立が行われる。

【0036】次に、信頼関係の確立が完了した後、無線通信装置1と無線通信装置2とが近距離通信回線10に

よって通信できない遠隔地において通信する場合について説明する。まず、無線通信装置1は、通信を行いたい相手側として、無線通信装置2の電子署名が付与された公開鍵23（以下、単に「公開鍵23」と称す）を指定して無線基地局3と広域ネットワーク19とを介して認証管理サーバ5に呼び出し要求を送信する。管理サーバ5は、無線通信装置1から送信された呼び出し要求先となる公開鍵23に対応する識別符号18を記憶部5-2から読み出して、読み出した識別符号18を広域ネットワーク19と無線基地局3を介して、無線通信装置1に送信する。

【0037】無線通信装置1は、認証管理サーバ5から受信した識別符号18を通信相手先として通信データに設定し、遠距離通信部130によって無線基地局3と広域ネットワーク19とを介して送信する。これにより、無線通信装置1から無線通信装置2に対して通信データが送信される。無線通信装置2についても同様に、上述した同様の手順に従い、無線通信装置1に対して通信データを送信することが可能である。

【0038】次に、無線基地局4から無線通信装置2に新たな識別符号18が発行される場合について説明する。無線通信装置2は、移動または通信の開始する場合に、新たな識別符号の発行要求を無線基地局4に行い、無線基地局4から発行される新たな識別符号18を受信し、記憶部140に記憶する。次いで、無線通信装置2は、新たな識別符号18を秘密鍵22によって電子署名し、公開鍵23とともに無線基地局4と広域ネットワーク19を介して認証管理サーバ5に送信して更新依頼をする。

【0039】認証管理サーバ5は、無線通信装置2から電子署名された新たな識別符号18と公開鍵23とを受信すると、電子署名された新たな識別符号18を確認した後、公開鍵23に対応する識別符号として記憶部5-2に記憶して更新する。これにより、以後、無線通信装置1から無線通信装置2に対する送信要求があった場合に、認証管理サーバ5から新たな識別符号18が無線通信装置1に送信されるので、識別符号18が更新されても、無線通信装置1と無線通信装置2とが通信を行うことができる。

【0040】以上説明した実施形態によれば、近距離通信回線10を介して公開鍵（公開鍵21、公開鍵23）を送受信するようにしたので、通信相手を視覚的に確認した相手だけが通信相手の公開鍵（公開鍵21または公開鍵23）を知り得ることができ、これにより、他の無線通信装置と識別することが可能である。また、無線通信装置1の利用者および無線通信装置2の利用者が互いに相手を視認した後に信頼関係の確立を行うことができる。

【0041】次に、上述の方法によって確立した信頼関係の失効について説明する。ここでは、無線通信装置1

と無線通信装置2との間において信頼関係の確立がなされている場合について説明する。無線通信装置1は、無線通信装置2に対する信頼関係が確立した関係を失効する要求である信頼関係失効要求を認証管理サーバ5に送信する。認証管理サーバ5は、無線通信装置1から無線通信装置2に対する信頼関係失効要求を受信すると、記憶部5-2に記憶された認証データから無線端末2の関係(識別符号18および公開鍵23)を削除し、広域ネットワーク19と無線基地局4とを介して無線通信装置2に公開鍵23の失効を送信する。

【0042】無線通信装置2は、認証管理サーバ5から公開鍵23の失効を受信すると、無線通信装置1に対応する秘密鍵22、共通鍵30を消去する。一方、無線通信装置1は、無線端末2に対応する公開鍵23、秘密鍵20、共通鍵30を記憶部140から消去する。このように、相互に信頼関係の確立を行った無線通信装置のいずれかの無線通信装置から認証管理サーバ5に信頼関係失効要求がなされることにより、確立された信頼関係が無効となる。

【0043】次に、第2の実施形態について説明する。この実施形態においては、イントラネットを移動体に拡張する場合について図2、図3、図6、図7を用いて説明する。図6において、無線通信装置1および無線通信装置2は、予め近距離通信回線10を用いて相互に自身に設定された識別子を送信し、上述した手順に従って相互に信頼関係の確立を行う。これにより、無線通信装置1において生成された公開鍵U1が無線通信装置2に通知され、無線通信装置2において生成された公開鍵U2が無線通信装置1に通知される。さらに、公開鍵U1、U2に対応する秘密鍵R1、R2はそれぞれ無線通信装置1、無線通信装置2内に記憶されている。

【0044】次に、無線通信装置2は、近距離通信回線10および遠距離通信回線とは別の通信回線60(イーサネット(登録商標)などのローカル・エリア・ネットワーク)を介してイントラネットL1に接続された他の装置(例えばサーバ、コンピュータ、プリンタなど)と通信可能に接続される。そして、無線通信装置2は、イントラネットを介して通信可能な機器のリストである機器リストK2(図7)を生成する。

【0045】一方、無線通信装置1は、近距離通信回線10のサービス圏外(通信可能な領域外)に移動した後、近距離通信部110によって(無線通信装置2に対する同じ通信回線でも別でもよい)を介して入出力端末D5に接続される。そして、無線通信装置1は、無線通信装置2に接続されているイントラネットL1上の機器に対して通信を行う指示が入出力端末D5から送信されると、無線基地局4、広域ネットワーク19と無線基地局4とを介して無線通信装置2から機器リストK2を取得する。これにより、入出力端末D5は、無線通信装置1にアクセスすることにより、無線通信装置2に接続さ

れている機器リストK2の紹介を行うことが可能となる。

【0046】次に、入出力端末D5は、使用者からの指示に応じて、機器リストK2の中から通信を行いたい相手側入出力機器を無線通信装置1に指示する。無線通信装置1は、無線通信装置2を介して、入出力端末D5から指示された相手側入出力機器と通信を確立し、入出力端末D5からの指示に応じて、相手側入出力機器とデータの送受信を行う。この場合、無線通信装置1は、無線通信装置2に送信するデータを公開鍵暗号手順(公開鍵U2を用いて暗号化してデータを送信する手順)を用いることにより、経路W3、無線基地局6、W4、W2間は、通信の傍受、改ざんに対して安全に通信を行うことが可能である。

【0047】次に、第3の実施形態の説明をする。この実施形態においては、信頼関係が確立されていない無線通信装置同士が、お互いに信頼関係の確立をしている機器を媒体として、信頼を確立する場合について図8を用いて説明する。この図において、無線通信装置1および無線通信装置2は、信頼関係を確立しており、無線通信装置1および無線通信装置D3は信頼関係を確立しているものとする。この状況下において、近距離通信回線10を用いた相互認証を行うことなく無線通信装置2と無線通信装置D3とが信頼関係を確立して、相互に通信を可能とする場合について説明する。

【0048】まず、無線通信装置2は、無線基地局D12を介して認証管理サーバ5に無線通信装置D3と共有可能な共通鍵Kaを生成するために必要な無線通信装置D3の識別情報の取得を依頼する。認証管理サーバ5は、認証データに基づいて、無線通信装置2と信頼関係を確立している無線通信装置群の中から無線通信装置D3と信頼関係の確立がなされている機器として無線通信装置1を検出する(この実施形態では無線通信装置1のみであるが、他に複数ある場合には、その中から適当にひとつを検出する)。

【0049】次に、認証管理サーバ5は、無線通信装置2に対し、無線通信装置2の識別符号を無線通信装置1に送信するべき指示を出す。次いで、この指示に応じて無線通信装置2から送信される無線通信装置2の識別符号を、記憶部5-2に記憶された無線通信装置1の公開鍵を用いて暗号化して無線通信装置1に送信するとともに、無線通信装置1に対し、受信した無線通信装置2の識別符号を無線通信装置D3に送信するべき指示を出す。

【0050】そして、この指示に応じて無線通信装置1から送信される無線通信装置2の識別符号を無線通信装置D3の公開鍵によって暗号化して無線通信装置D3に送信するとともに、無線通信装置D3に対し、無線通信装置D3の識別符号を無線通信装置1に送信する指示を出す。

【0051】そして、この指示に応じて無線通信装置3から送信される無線通信装置D3の識別符号を無線通信装置1の公開鍵によって暗号化して無線通信装置1に送信するとともに、無線通信装置1に対し、無線通信装置D3の識別符号を無線通信装置2に送信する指示を出す。

【0052】そして、この指示に応じて無線通信装置1から送信される無線通信装置D3の識別符号を無線通信装置2の公開鍵によって暗号化して無線通信装置2に送信する。

【0053】上述のようにして、無線通信装置2と無線通信装置D3との間において、識別符号交換を遠距離通信回線を用いて間接的に行うことにより、近距離通信回線10を用いることなく、無線通信装置2と無線通信装置D3との間における信頼関係を確立することができる。以降の手順は、上述した実施形態と同様に行われる。この実施形態によれば、信頼を確立していない機器同士が、お互いに信頼を確立している機器を媒体として、信頼を確立するようにしたので、近距離通信回線10を使用できる領域内に接近することなく、信頼関係を

確立することができる。

【0054】以上説明した実施形態によれば、万が一、識別符号（IPアドレス）自体が単体で漏洩した場合においても、そのIPアドレスが誰のものかは把握できないので、特定の相手を対象としてIPアドレスが悪用される危険性を低減させることができる。

【0055】なお、上述した実施形態では、第1の通信回線としてBLUETOOTHを適用した場合について説明したが、BLUETOOTHを電話回線に換えて、信頼関係の確立を行うようにしてもよい。これにより、無線通信装置1の利用者と無線通信装置2の利用者とが視認できる距離に近づくことなく、また、共通の信頼関係を確立した無線通信装置を介することなく、信頼関係の確立を行うことが可能である。この場合、無線通信装置の利用者が、予めお互いに会っておく、または、電話を介して相手の確認をする等、確認作業をしておくことによって、通信相手を把握することができ、信頼性を向上させることができる。

【0056】また、上述した実施形態における無線通信装置と端末（例えば、端末1-n、端末2-n、入出力端末D5）とを同一筐体内に設けるようにしてもよい。これにより、無線通信装置と端末とを別々に製造する場合に比べて製造コストを低減させて、各種データを送受信することができる効果が得られる。

【0057】また、上述した実施形態において、電子署名付の公開鍵を交換することにより、無線通信装置1と無線通信装置2との間において信頼関係の確立を行うようにしたが、電子署名が付与されていない状態の公開鍵を相互に交換して信頼関係の確立を行うようにしてもよい。

【0058】また、上述した共通鍵30を生成する場合に、識別子11、識別子12として識別符号17、識別符号18を用いるようにしてもよい。また、通信回線を2経路以上使用して、相手側となる無線通信装置の登録や、データの送受信を行うようにしてもよい。

【0059】また、図1における無線通信装置1（2、3）、認証管理サーバ5の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより通信を行ってもよい。なお、ここでいう「コンピュータシステム」とは、OSや周辺機器等のハードウェアを含むものとする。また、「コンピュータシステム」は、WWWシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フロッピー（登録商標）ディスク、光磁気ディスク、ROM、CD-ROM等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであっても良く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであっても良い。

【0060】以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【0061】

【発明の効果】以上説明したように、この発明によれば、第1の通信回線を用いて通信相手となる無線通信装置の登録に関する通信を行い、第1の通信手段によって登録された通信相手に対し、第1の通信回線と異なる通信回線を用いて通信を行う第2の通信手段とを設けたので、識別符号を第3者に知られないように通信相手に通知することができる効果が得られる。

【0062】また、この発明によれば、近距離において通信を行う相手側となる無線通信装置の登録を行うようにしたので、無線通信装置の利用者が互いに相手を視認した後に信頼関係の確立を行うことができ、これにより、利用者同士が通信相手を把握した上で通信を行うことができる効果が得られる。

【0063】また、この発明によれば、信頼を確立していない機器同士が、お互いに信頼を確立している機器を

媒体として、信頼を確立するようにしたので、無線通信装置の利用者同士が接近することなく、信頼関係を確立することができる。

【0064】また、この発明によれば、第1の通信回線を介して識別子を送信しておき、第2の通信回線を介して固有情報によって通信する相手側を指定するようにしたので、識別符号自体が単体で漏洩した場合には、そのIPアドレスが誰のものは把握できないので、特定の相手を対象としてIPアドレスが悪用される危険性を低減させることができる。

【図面の簡単な説明】

【図1】 この発明の一実施形態による無線通信装置、認証サーバを適用した通信システムの構成を示す概略ブロック図である。

【図2】 無線通信装置1の構成を示す概略ブロック図である。

【図3】 認証管理サーバ5の構成を示す概略ブロック図である。

【図4】 図1の構成における通信システムの動作を説明するための図面である。

【図5】 認証管理サーバ5の記憶部5-2に記憶される認証データを示す図面である。

【図6】 他の実施形態における通信システムの動作を説明するための図面である。

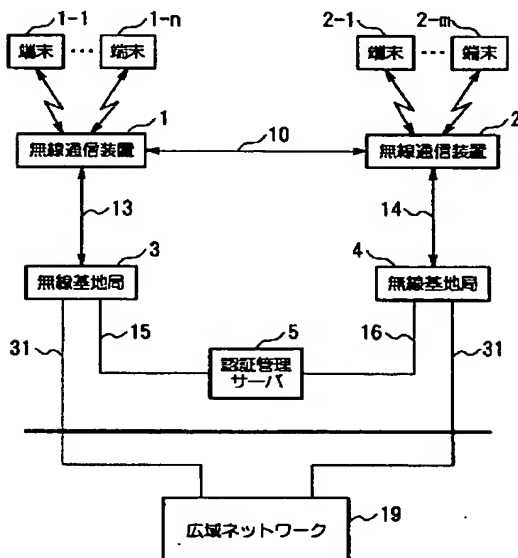
【図7】 機器リストK2の一例を示す図面である。

【図8】 他の実施形態における通信システムの動作を説明するための図面である。

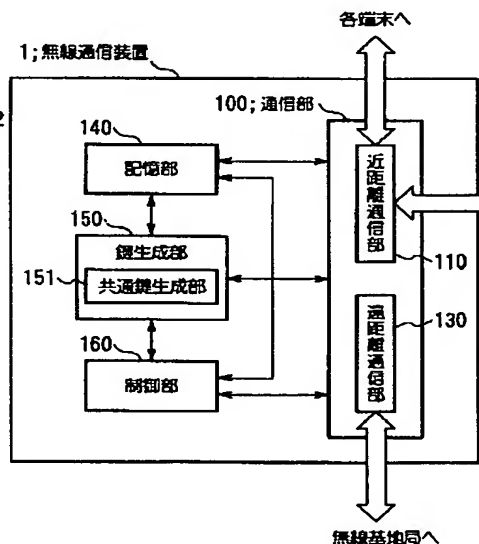
【符号の説明】

1、2、D3	無線通信装置	3、4	無線基地局
5	認証管理サーバ	5-1	通信部
5-2	記憶部	5-3	制御部
10	10 近距離通信回線	11、12	識別子
13、14、15、16	通信回線	17、18	識別符号
19	ネットワーク	19	広域
20、22	秘密鍵	21、23	公開鍵
30	共通鍵	100	通信部
110	近距離通信部	130	遠距離通信部
140	記憶部	150	鍵生成部
151	共通鍵生成部	160	制御部
151	共通鍵生成部	160	制御部

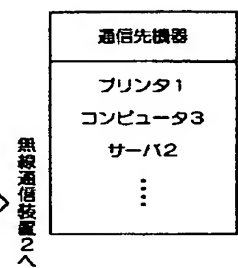
【図1】



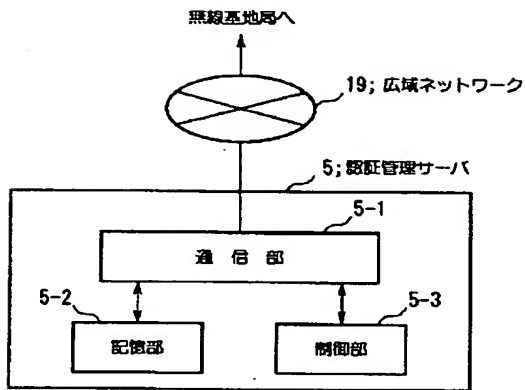
【図2】



【図7】



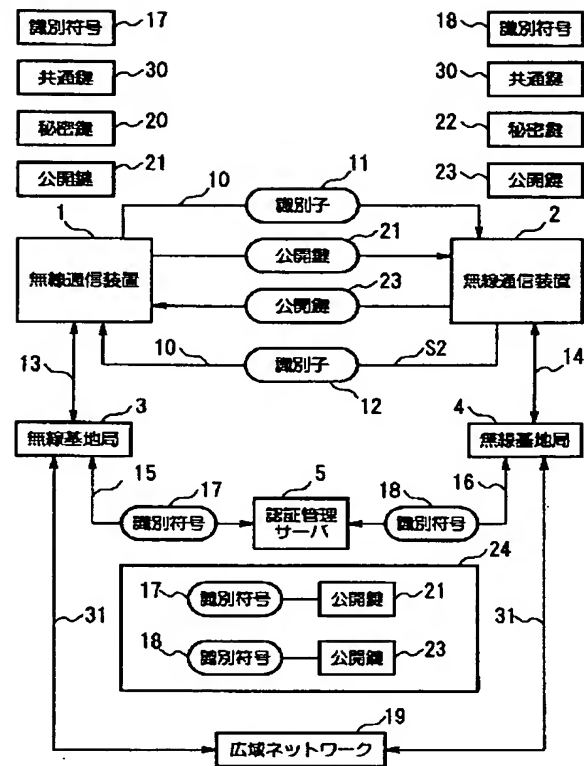
【図3】



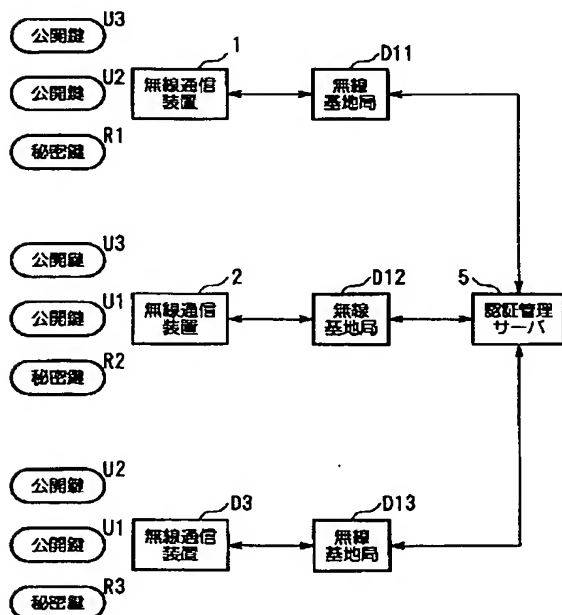
【図5】

識別符号	公開鍵	信頼関係の確立
識別符号 17	公開鍵 21	無線通信装置 2
識別符号 18	公開鍵 23	無線通信装置 1
⋮	⋮	

【図4】



【図8】



【図6】

